Phishing

“Phishing (also known as carding and spoofing) is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords. “

http://en.wikipedia.org/wiki/Phishing
Phishing – In the Beginning

• In the early 1990s unethical AOL users created false accounts with “algorithmically generated credit card numbers — these accounts could last weeks or even months until new ones were required.
  – At this point in time AOL was a parallel service to the Internet
  – AOL eventually brought in measures in late 1995 to prevent this, so early AOL crackers resorted to phishing for legitimate AOL accounts.”

• Individuals involved in such measures were often those involved in illegal sale and distribution of bootleg software.

• http://en.wikipedia.org/wiki/Phishing
Phishing – In the Beginning

• The phisher or cracker would “pose as an AOL staff member and send an instant message to a potential victim, asking the victim to reveal his or her password.”
http://en.wikipedia.org/wiki/Phishing#Early_phishing_on_AOL

• The phisher would use the … common technique of sending some kind of message to the unsuspecting AOL user asking to give “up sensitive information … include text such as "verify your account" or "confirm billing information". Once the victim had submitted his or her password, the attacker could then access the victim's account and use it for various criminal purposes, such as spamming.”
Phishing – Moving on from AOL

• In 1997 AOL adjusted its security policies making it very difficult for such illegal activities to occur. As a result these activities migrated elsewhere on the Internet.
• Phishing is now unfortunately **Everywhere**!
• Losses from phishing in the US alone (businesses and individuals) are estimated in the billions of dollars annually and impact millions of people.
Phishing

USER FRIENDLY by J.D. "Iillad" Frazer

DEAR LUCRE INTERNET BANK CLIENT,

DUE TO A MINOR BUG IN OUR BANKING SOFTWARE, WE HAVE RESET YOUR LOGIN AND PASSWORD TO BLANK VALUES. PLEASE VISIT OUR SITE AND ENTER YOUR NAME, NEW LOGIN, AND NEW PASSWORD AND YOU WILL HAVE ACCESS TO YOUR ACCOUNT ONCE MORE.

THANK YOU,
F. LUCRE, C.E.O.

stef murky ←
smurky ←
butter-parkay ←

YOU DON'T REALLY HAVE MUCH MONEY IN CHEQUING, DO YOU.

WAIT A SECOND, SOMETHING'S NOT QUITE RIGHT...

http://www.userfriendly.org/static/

Copyright © 2008 by Helene G. Kershner
Phishing

Examples
- Fake sites that look real are called **spoofed** websites.
- Look for typos
Phishing

• What is identity theft?
Phishing Examples

Emails that say:
• Verify your account information
• You have just won!
• If you fail to respond within 36 hours your account will be closed


http://www.youtube.com/watch?v=sqRZGhiHGxg  
http://www.youtube.com/watch?v=Ao20tAS3x3I (very cute by Symantec)  
http://www.youtube.com/watch?v=e_TALggP0xQ (home)  
http://www.youtube.com/watch?v=tR64APeWACg&NR=1 (office)
Subject: EMAIL ACCOUNT MAINTENANCE
From: CAMPUS WEB EMAIL TECHNICAL SERVICE info@webteam.com
Reply-To: techservice1@live.com
Date: 10/29/2008 3:50 PM

Dear Buffalo e-mail User,

A Computer Database Maintainance is currently going on. This Message is Very Important. We are very concerned with stopping the proliferation of spam. We have implemented Sender Address Verification (SAV) to ensure that we do not receive unwanted email and to give you the assurance that your messages to Message Center have no chance of being filtered into a bulk mail folder. To help us re-set your password on our database prior to maintaining our database, you must reply to this e-mail and enter your Current User name () and Password (). Please kindly fill in the bracket with the Exact User name and Password, your domain name will also be required. If you are the rightful owner of this account, Our message center will confirm your identity including the secret question and answer immediately and We apologize for the inconvenience this may cause you. We assure you more quality service at the end of this maintenance. The Buffalo Campus Web Email Software is a fast and light weight application to quickly and easily accessing your e-mail. Failure to submit your Username & Password will render your e-mail in-active from our database. Thank you for using Buffalo Web Email! WEBMAIL TECHNICAL ADMIN

https://www.buffalo.edu

cse@buffalo
All,

Some CSE faculty and staff are wondering if this message is legitimate. In fact, it is spam designed to harvest and exploit your personal information.

As a general rule, if you ever receive email that asks for your password, it's malicious spam and you should ignore it. UBIT (and your bank, credit card company, mortgage holder, etc.) will never ask you for your password via email.

Other red flags in this message include:

1. The message purports to be from a UB database administrator, but it originates from an email address outside the buffalo.edu domain. UBIT policy dictates that official correspondence must originate from UBITName@buffalo.edu addresses.
2. The message is poorly written and ungrammatical. UBIT personnel are usually pretty good about proofreading.
3. The message's content attempts to sound official and jargon-y but is ultimately without meaning or substance.

Yours in healthy skepticism,
Fraudulent E-mail Examples

Phishing

• http://www.antiphishing.org/
Phishing

- Not just an email issue
  - MySpace Introduces Anti-Phishing measures
    http://mashable.com/2008/02/11/myspace-anti-phishing/
Phishing

How to avoid Phishing Scams

• **Suspect any email that asks for personal or financial information**
• Don’t use **links** in web pages, IMs, or chats that you suspect or where you don’t know the sender.
• Avoid filling out email forms that ask for personal or financial info
• Make sure you’re using a **secure website** when submitting credit card or other sensitive info from your web browser.
• **Look for the security lock** and http://
  – scam sites may not use these.
  – Check to see that the address the return email quotes is the same thing as the website address

Copyright © 2009 by Helene G. Kershner
Phishing

How to avoid Phishing Scams

- Consider installing a fraud catching web browser tool bar to help protect you from known sites
  - IE 7 and FireFox 2 include such a feature
  - Earthlink ScamBlocker is such a tool
- Regularly check your online accounts, don’t leave such accounts untouched for months
- Regularly check your bank, credit card and debit account statements and check for illegal use
  - Issues with debit cards
- Keep your browser updated
- Report “phishing” por “Spoofed” emails
Phishing

• What can be done?
  – Educate users
  – Make pages more difficult to “spoof”
  – Anti-phishing software
  – “smart” - spam filters
  – Legislation
  – Industry/government/law enforcement working groups
The FTC suggests

- **If you get an email or pop-up message that asks for personal or financial information, do not reply.** And don’t click on the link in the message, either.

- **Area codes can mislead.** Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a “refund.” Because they use Voice Over Internet Protocol technology, the area code you call does not reflect where the scammers really are.
Behind the Machine: Phishing

• Don’t email personal or financial information if requested by a message to you!
• Look for indicators that the site is secure, like a lock icon on the browser’s status bar or a URL for a website that begins “https:” (the “s” stands for “secure”). Unfortunately, no indicator is foolproof; some phishers have forged security icons
• Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.

http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm

Copyright © 2008 by Helene G. Kershner